TẤN CÔNG GIAO THỨC TCP/IP, CÁC CÔNG CỤ PHÒNG THỦ VÀ BẢO MẬT

Conference Paper · December 2015

CITATIONS
0

READS
14,003

1 author:

Giang Nguyen Hong
TCU, Vietnam
7 PUBLICATIONS **30** CITATIONS

SEE PROFILE

TẤN CÔNG GIAO THỨC TCP/IP, CÁC CÔNG CỤ PHÒNG THỦ VÀ BẢO MẬT

Trần Thanh Phương, Lê Văn Cường, Phan Xuân Tuấn, Nguyễn Hồng Giang, Hà Văn Muôn
Đai học Thông tin Liên lạc
Email: {Tranthanhphuong7772@gmail.com, giang225256@yahoo.com.vn, muon.ha@mail.ru}

***Tóm tắt*—TCP/IP (Transmission Control Protocol/ Internet Protocol) là bộ giao thức cho phép kết nối các hệ thống mạng không đồng nhất với nhau. Ngày nay, TCP/IP được sử dụng rộng rãi trong các mạng cục bộ cũng như trên mạng Internet toàn cầu. Tuy nhiên, TCP/IP là một giao thức mở nên các hacker có thể tìm thấy những lỗ hổng của nó một cách dễ dàng bằng cách thử nhiều kiểu tấn công khác nhau [1]. Nhiều cuộc tấn công nhằm vào bộ giao thức TCP/IP bao gồm cả các cuộc tấn công giả mạo, tấn công từ chối dịch vụ, tấn công xác thực định tuyến ... Các công cụ khác nhau đã được thiết kế để phân tích và xác định sự có mặt của các lỗ hổng và cách thức thực hiện khai thác chúng trong bộ giao thức TCP/IP. Trong bài báo này, chúng tôi xin giới thiệu một số phương thức và công cụ tấn công và phòng thủ cho bộ giao thức TCP/IP như tường lửa, hệ thống phát hiện xâm nhập, phân tích giao thức, nghe lén và quét lỗ hổng.**

***Từ khóa* — Công cụ tấn công mạng, An ninh mạng**

I. GIỚI THIỆU

Tên TCP/IP liên quan đến hai giao thức quan trọng nhất trong bộ giao thức - Giao thức kiểm soát truyền tải (Transmission Control Protocol - TCP) và Giao thức Internet (Internet Protocol - IP) [2].

A. Giao thức IP

Nhiệm vụ chính của giao thức IP là cung cấp khả năng kết nối các mạng con thành liên kết mạng để truyền dữ liệu, vai trò của IP là vai trò của giao thức tầng mạng trong mô hình OSI. Giao thức IP là một giao thức kiểu không liên kết (connectionlees) có nghĩa là không cần có giai đoạn thiết lập liên kết trước khi truyền dữ liệu.

Khi giao thức IP được khởi động nó trở thành một thực thể tồn tại trong máy tính và bắt đầu thực hiện những chức năng của mình, lúc đó thực thể IP là cấu thành của tầng mạng, nhận yêu cầu từ các tầng trên nó và gửi yêu cầu xuống các tầng dưới nó. Đối với thực thể IP ở máy nguồn, khi nhận được một yêu cầu gửi từ tầng trên, nó thực hiện các bước sau đây:

• Tạo một IP datagram dựa trên tham số nhận được.

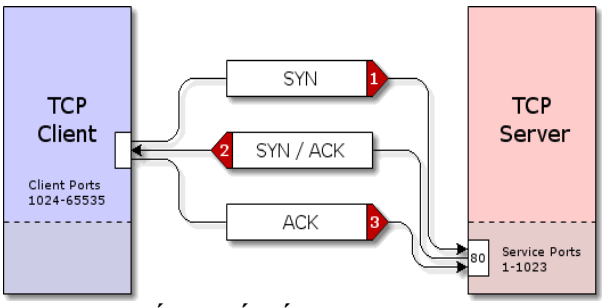
• Tính checksum và ghép vào header của gói tin.

• Ra quyết định chọn đường: hoặc là trạm đích nằm trên cùng mạng hoặc một gateway sẽ được chọn cho chặng tiếp theo.

• Chuyển gói tin xuống tầng dưới để truyền qua mạng.

B. Giao thức điều khiển truyền dữ liệu TCP

TCP là một giao thức "hướng kết nối" (connection oriented), nghĩa là cần phải thiết lập liên kết giữa hai thực thể TCP trước khi chúng trao đổi dữ liệu với nhau. Giữa client và server muốn thực hiện kết nối để trao đổi thông tin thì chúng phải thực hiện qua ba bước sau (cơ chế bắt tay ba bước) như Hình 1.



Hình 1. Thiết lập kết nối TCP giữa client và server

• Bước 1: Client gửi gói tin SYN tới server thông báo yêu cầu thiết lập kết nối. Lúc này một kết nối tiềm tàng (potential connection) đã được thiết lập giữa client và server.

• Bước 2: Server sau khi nhận được tín hiệu SYN trên sẽ gửi lại cho client gói tin SYN/ACK xác nhận việc thiết lập liên kết.

• Bước 3: Client sau khi nhận được gói tin SYN/ACK trên, nó sẽ gửi tiếp cho Server gói tin ACK. Kết thúc bước này giữa client và server đã hoàn thành một kết nối.

với **SYN**: là một bit cờ trong gói tin TCP/IP dùng đế thông báo bắt đầu kết nối, **ACK**: là một bit cờ trong gói tin TCP/IP của bên nhận gửi cho bên gửi để thông báo đã nhận được gói tin, **SEQ**: là số thứ tự của gói tin.

II. TẤN CÔNG TCP/IP

A. Tấn công TCP Syn Flood

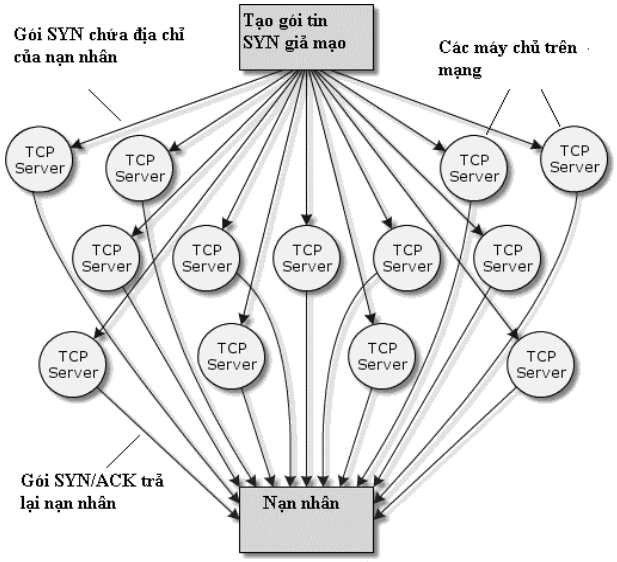
Kiểu tấn công TCP SYN flood là một kiểu tấn công trực tiếp vào máy chủ bằng cách tạo ra một số lượng lớn các kết nối TCP nhưng không hoàn thành các kết nối này. Hacker sử dụng cơ chế bắt tay ba bước trong quá trình thiết lập kết nối giữa hai thực thể TCP. Máy hacker sử dụng một địa chỉ giả mạo và gửi hàng loạt bản tin yêu cầu kết nối tới máy tính nạn nhân với bit SYN được bật (bước 1), khi đó nạn nhân nhận được gói tin này ngay lập tức nó sẽ dành một phần bộ nhớ cho kết nối này, máy tính nạn nhân nhận được yêu cầu trên thì trả lời lại với bản tin bit ACK, SEQ được bật (bước 2) và chờ để hacker trả lời, nhưng hacker không trả lời điều này sẽ làm cho máy tính nạn nhân luôn ở trong tình trạng chờ và dần dần sẽ cạn kiệt tài nguyên không thể phục vụ được nữa [3].

B. Giả mạo địa chỉ IP (IP Spoofing)

Địa chỉ IP giả mạo liên quan đến việc tạo ra các gói TCP/IP sử dụng địa chỉ IP giả với mục đích để che giấu danh tính hoặc giả mạo danh tính chủ sở hữu của địa chỉ IP được sử dụng [4]. Hành vi này có thể thực hiện các cuộc tấn công khác nhau như sau:

• Tấn công từ chối dịch vụ (Denial of Service Attack-DoS): Hacker có thể gửi một số lượng lớn các gói tin yêu cầu kết nối (SYN) tới máy nạn nhân mà không cần quan tâm phản hồi (ACK) vì Hacker sẽ không nhận được bất kỳ gói tin phản hồi từ các nạn nhân [5]. Tất cả gói phản hồi sẽ được hướng tới các địa chỉ IP giả mạo. Ngoài ra, danh tính của kẻ tấn công cũng sẽ không được tiết lộ. Cuộc tấn công này làm cho nạn nhân bị loại khỏi dịch vụ.

• Tấn công từ chối dịch vụ phản xạ nhiều vùng (Distributed Reflection DOS- DRDoS): Mục tiêu chính của DRDoS là chiếm đoạt toàn bộ băng thông của máy nạn nhân, làm tắc nghẽn hoàn toàn đường kết nối từ máy nạn nhân vào xương sống của Internet và làm tiêu hao tài nguyên. Trong suốt quá trình máy nạn nhân bị tấn công bằng DRDoS, không một máy khách nào có thể kết nối được vào máy nạn nhân đó, tất cả các dịch vụ chạy trên nền TCP/IP như: DNS, HTTP, FTP, POP3, ... đều bị vô hiệu hóa. Hacker sử dụng các server phản xạ, hacker sẽ gửi yêu cầu kết nối (SYN) tới các server có bandwidth rất cao trên mạng – server phản xạ, các gói tin yêu cầu kết nối này mang địa chỉ IP giả - chính là địa chỉ IP của máy nạn nhân. Các server phản xạ này gửi lại máy nạn nhân các gói SYN/ACK dẫn tới hiện tượng nhân băng thông – bandwidth multiplication (Hình 2).



Hình 2. Tấn công kiểu DRDoS.

• Tấn công môi trường xác thực bằng địa chỉ IP: Là tấn công môi trường xác thực dựa trên địa chỉ IP. Trong trường hợp mạng nội bộ, xác thực bằng địa chỉ IP, không cần một tên đăng nhập hoặc mật khẩu để truy cập [6]. Hacker có thể giả địa chỉ IP để có được quyền truy cập trái phép vào máy tính nạn nhân mà không xác thực..

• Kiểu tấn công người đứng giữa (Man in The Middle Attack): Nó liên quan đến việc hack một phiên liên lạc được xác thực giữa hai máy tính A và B. Hacker sau khi hoàn thành các bước xác thực sẽ giả mạo địa chỉ IP của một nạn nhân A hoặc B đã được xác thực và nhận được các gói tin qua lại giữa hai máy A và B [7].

Các biện pháp bảo vệ chống lại tấn công IP Spoofing được đưa ra sau đây [8].

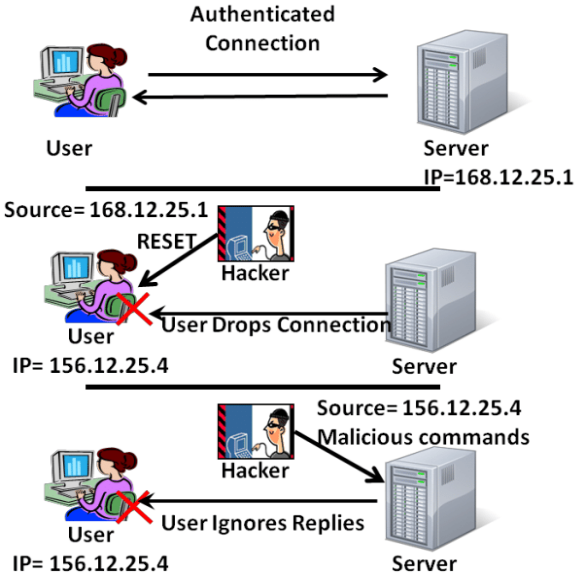
• Dùng mật mã xác thực: Nếu cả hai đầu của cuộc nói chuyện đã được xác thực, khả năng tấn công theo kiểu Man-in-the-Middle Attack có thể được ngăn chặn. Mã hoá traffic giữa các thiết bị (giữa 2 router, hoặc giữa 2 hệ thống đầu cuối và router) bằng một IPSec tunnel.

• Dùng danh sách kiểm tra truy cập Access Control List (ACL) trên các interface của router. Một ACL có thể được dùng để loại bỏ những traffic từ bên ngoài mà lại được đóng gói bởi một địa chỉ trong mạng cục bộ khi bị lôi cuốn vào một cuộc tấn công DDoS.

• Bộ lọc các gói dữ liệu: Điều này ngăn chặn các gói tin gửi đến, chúng không đáp ứng các tiêu chí chính sách bảo mật, như các yêu cầu ping từ bên ngoài mạng được lọc. Tương tự như vậy, gói tin đi ra cũng có thể được lọc dựa trên tiêu chí địa chỉ cổng, IP của nguồn hoặc đích.

• Sử dụng lớp trên: Kết hợp cơ chế phòng vệ ở tầng trên có thể ngăn chặn IP giả mạo như sử dụng số thứ tự trong trường số thứ tự của gói tin TCP ở tầng giao vận như vậy kẻ tấn công phải đoán được số thứ tự cũng trước khi giả mạo gói tin.

C. Hack kết nối (Connection Hacking)



Hình 3. Hack phiên liên lạc.

Xác thực giữa User và Server diễn ra trong giai đoạn đầu thiết lập kết nối. Từ đó không có yêu cầu xác nhận. Như Hình 3, hacker có thể lợi dụng điều này bằng cách giả mạo địa chỉ IP của Server (`168.12.25.1`) gửi một thiết lập lại cho User và sau đó hacker tiếp tục giả mạo địa chỉ IP của User (`156.12.25.4`) tiếp tục phiên làm việc với Server bằng sử dụng địa chỉ IP giả mạo [9]. Một cách khác của việc hack phiên liên lạc là Hacker có thể ăn cắp tập tin cookie được lưu trữ trên máy nạn nhân hoặc có được cookie của máy nạn nhân bằng cách nghe lén (Sniffer) các gói tin trên mạng không được mã hóa. Sau đó, những cookie có thể được sử dụng với các Web server để thiết lập một phiên xác thực. Các biện pháp phòng chống hack kết nối được chỉ ra trong [8] như sau:

• Mã hóa: Mã hóa bảo đảm cho việc trao đổi gói tin giữa User và Server không bị Hacker đọc được nội dung và cũng không thể sử dụng chúng cho việc cướp quyền.

• Sử dụng tái xác thực: Yêu cầu xác thực định kỳ sau một thời gian nhất định.

ISBN: 978-604-62-4226-0

D. Tấn công giao thức định tuyến RIP

Routing Information Protocol (RIP) là một giao thức định tuyến được sử dụng trong bộ giao thức TCP/IP để định tuyến các gói dựa trên số chặng (hop). Trước khi đưa ra quyết định định tuyến RIP đếm số bước nhảy trên mọi hướng có thể và chọn đường đi tới đích có số bước nhảy ngắn nhất. Giá trị đếm hop tối đa có thể là 15 hop và bất cứ trường hợp nào lớn hơn 15 được coi là vô hạn. Cơ chế này được sử dụng để trách gói tin rơi vào vòng lặp. Phiên bản chuẩn của RIP không có phần xác thực. Thông tin cung cấp trong bản tin RIP thường được sử dụng mà không có sự kiểm tra xác thực lại chính nó. Hacker có thể giả mạo 1 bản tin RIP, ví dụ xác định máy X có tuyến ngắn nhất ra ngoài mạng. Như vậy, mọi gói tin gửi ra từ mạng này sẽ được định tuyến qua X và máy X có thể kiểm soát, sửa đổi gói tin [10]. Để phòng chống lại tấn công giao thức RIP, sử dụng một số biện pháp theo [8].

• Sử dụng thuật toán xác thực mật khẩu đơn giản, làm cho việc tấn công qua RIP khó khăn hơn.

• Giải pháp IPsec VPN cũng cung cấp khả năng mã hóa thông tin định tuyến qua các routers sử dụng IPsec VPN.

• Các gói dữ liệu được lọc dựa trên mã nguồn và đích.

• Phân tích nhật ký (log) thường xuyên nhằm phát hiện bất thường.

• Kiểm tra các đường truyền trước khi chấp nhận

E. Tấn công tràn ngập gói tin ICMP

Giao thức Internet Control Message Protocol (ICMP) thực hiện truyền các thông báo điều khiển (báo cáo về tình trạng lỗi trên mạng ...) giữa các gateway hay các trạm của liên mạng. Tình trạng lỗi có thể là: một datagram không thể tới được đích của nó, hoặc một router không đủ bộ đệm để lưu và chuyển một datagram.

Ping là một chương trình dùng để báo cho người sử dụng biết hai host trên mạng có thông với nhau không. Ping dựa trên giao thức ICMP. Nó cho phép người sử dụng gửi các gói tin tới một hệ thống ở xa và hiển thị khoảng thời gian từ khi gửi gói tin đến khi nhận được phản hồi từ phía nhận (Round Trip Time: RTT). Gói tin được gửi đi là ICMP echo request, gói tin phản hồi là ICMP echo receive. Hacker sẽ sử dụng giao thức ICMP này để tấn công nạn nhân theo cách sau:

• Bước 1: Kẻ tấn công giả mạo là nạn nhân, gửi đi một lệnh Ping với địa chỉ IP là của nạn nhân và địa chỉ đích là dạng broadcast của một mạng nào đó. Sau bước này tất cả các host trong mạng `10.0.0.x` sẽ nhận được gói tin ICMP từ host của nạn nhân.

• Bước 2: Do sự nhầm lẫn như trên mà tất cả các host trong mạng `10.0.0.x` đều gửi về cho nạn nhân một gói tin ICMP echo receive. Hàng loạt các gói tin dạng này là nguyên nhân gây lên hện tượng làm băng thông tới host của nạn nhân bị chiếm dụng. Nạn nhân sẽ không thể giao dịch với các host khác trên mạng.

Phòng chống lại các cuộc tấn công ICMP có bằng các biện pháp sau đây:

• Đối với các firewall cứng, kích hoạt cơ chế ICMP Flooding Protection.

• Đối với các firewall mềm trên linux như iptables, có thể sử dụng luật sau:

```
# iptables –A INPUT –p icmp –m limit
–limit 2/second –limit-burst 2 –j ACCEPT
```

• Đối với hệ điều hành window, chặn toàn bộ các gói tin ping bằng cách sử dụng lệnh sau trên cmd:

```
# netsh firewall set icmpsetting type
all mode disable
```

F. Tấn công giả mạo DNS(DNS Snoffing Attack)

Domain Name System (DNS) là một dịch vụ được sử dụng trong lớp ứng dụng để ánh xạ một địa chỉ IP sang một tên miền và ngược lại [11]. Tấn công giả mạo DNS liên quan tới nhiễm độc bộ nhớ đệm DNS (DNS cache poisoning), hay còn được gọi là giả mạo DNS, là một kiểu tấn công khai thác lỗ hổng trong hệ thống tên miền (DNS – domain name system) để chuyển hướng lưu lượng truy cập Internet từ máy chủ hợp pháp tới các máy chủ giả mạo. Cách phòng chống giả mạo DNS được đề cập [11].

• Sử dụng xác thực dựa trên địa chỉ IP thay vì dựa trên tên miền.

• Sử dụng mã hóa để ngăn chặn giả mạo DNS.

III. CÔNG CỤ BẢO MẬT TCP/IP

A. Nghe lén mạng (Network Sniffer)

Nghe lén mạng-Sniffing là công cụ, phần mềm hoặc phần cứng, được các quản trị viên dùng theo dõi, chuẩn đoán, phát hiện các sự cố mà không thay đổi hoặc chuyển hướng các gói tin nhằm giúp cải thiện hoạt động hệ thống mạng.

• Wireshark: là một công cụ nghe lén mã nguồn mở được sử dụng để phân tích các gói tin [12]. Nó bắt các gói tin trực tiếp, và có thể phân tích chúng trong chế độ offline. Các gói này có thể bao gồm Ethernet, IEEE 802.11, PPP, và loopback. Wireshark có thể làm việc trên nhiều nền tảng như Windows, Linux, OS X, Solaris, NetBSD, FreeBSD. Nó cung cấp giao diện đồ họa và giao diện dòng lệnh.

• Tcpdump: là phần mềm miễn phí được sử dụng để phân tích các gói tin TCP/IP bằng cách sử dụng giao diện dòng lệnh. Công cụ này hoạt động chủ yếu trên Linux, nhưng cũng có thể làm việc trên các hệ điều hành khác như Solaris, BSD, HP-UX, AIX và Windows thông qua WinDump [13].

• Kismet: không chỉ là công cụ phân tích gói tin mà còn là một hệ thống phát hiện xâm nhập (IDS). Nó có thể bắt các gói tin trên mạng không dây sử dụng chuẩn 802.11a/b/g/n, các kết quả được hiển thị bằng cách sử dụng giao diện dòng lệnh. Kismet được viết bằng C ++ và có thể làm việc trên các hệ điều hành Linux, Solaris, BSD, Mac OS X, HP-UX và AIX [14].

• Ettercap: là một công cụ khai thác và tấn công trên mạng LAN. Nó có khả năng dò tìm tất cả các máy và tiến hành nghe lén, đây là một công cụ không thể thiếu khi tấn công một mạng LAN. Nó làm việc trên nhiều nền tảng như Microsoft Windows, Linux, Mac OS X, BSD và Solaris [15].

B. Các công cụ quét lỗ hổng

Các công cụ quét lỗ hổng được sử dụng để tìm các lỗ hổng trên mạng máy tính, hệ thống máy tính, hoặc các ứng dụng máy tính. Những công cụ này được sử dụng bởi Hacker để tìm thấy lỗ hổng và khai thác chúng. Mặt khác, các quản trị viên cũng sử dụng nó để tìm lỗ hổng bảo mật trên hệ thống của họ

để khắc phục ngăn chặn các cuộc tấn công. Sau đây là một số công cụ thường được sử dụng.

• Nessus: là một công cụ quét lỗ hổng mã nguồn mở và miễn phí cho đến năm 2005. Sau đó, nó được chuyển đổi thành một sản phẩm thương mại. Nessus hoạt động bằng cách phân tích mạng để tìm lỗ trong mạng. Nó là một công cụ đa nền tảng chạy trên các hệ điều hành như Linux, Mac OS X và Microsoft Windows. Nó sử dụng giao diện đồ họa, thân thiện với người sử dụng [16].

• OpenVAS: OpenVAS là một công cụ quét lỗ hổng bảo mật mạnh mẽ được tích hợp trên hệ điều hành Backtrack dành cho các nhà quản trị. Hiện nay OpenVAS đã quét hơn 25.000 lỗ hổng. Công cụ này được tạo ra như một nhánh của Nessus khi Nessus trở nên thương mại hóa [17].

• Core Impact: là một công cụ để khai thác các lỗ hổng hơn là tìm kiếm các lỗ hổng. Nó có khả năng tự động cập nhật những cách khai thác lỗ hổng bảo mật (Exploits), cùng với một đội ngũ các nhà bảo mật chuyên nghiệp viết lên các đoạn Exploit, nó là một sản phẩm thương mại [18].

• Retina: là một công cụ quét lỗ hổng được sử dụng để tra cứu các lỗ hổng trên hệ thống mạng, sử dụng giao diện đồ họa. Nhược điểm của công cụ này là nó chỉ hoạt động trên Microsoft Windows và là một công cụ thương mại [19].

C. Công cụ phát hiện tấn công

Một số công cụ được sử dụng để phát hiện các cuộc tấn công nhưng chúng không thể ngăn chặn các cuộc tấn công. Loại công cụ này được gọi là hệ thống phát hiện xâm nhập Intrusion Detaction System (IDS) và một thể loại cụ thể của IDS chỉ hoạt động ở lớp mạng và được gọi là Network Intrusion Detection System (NIDS). Một số IDS đáng chú ý được liệt kê dưới đây:

• Firestorm: Hệ thống pháthiện xâm nhập mạng này có hiệu suất cao và có đầy đủ khả năng để phát hiện các cuộc tấn công khác nhau. Nó có thể phân tích nhiều giao thức để phát hiện bất kỳ các mẫu độc hại trong lưu lượng mạng [21]. Nó sử dụng phương pháp phát hiện bất thường và hỗ trợ đầy đủ quy tắc Snort [20]. Firestorm chạy trên các nền tảng Linux 2.x, FreeBSD 4.x, OpenBSD, và Solaris.

• Prelude: là một IDS lai, trong đó sử dụng các quy tắc Snort và có khả năng sử dụng các quy tắc IDS khác. Nó sử dụng một số cảm biến trong mạng để nắm bắt và phát hiện bất kỳ gói tin độc hại. Nó có thể làm việc trên Linux, BSD, và hệ điều hành khác [22].

• Dragon: là hệ thống phát hiện xâm nhập mạng và máy trạm. Nó là một công cụ thương mại và đi kèm với thư viện phong phú, nó cho phép nó phát hiện một loạt các cuộc tấn công độc hại. Nó có giao diện đồ họa thân thiện với người dùng và cả giao diện dòng lệnh [23].

• Bro: là một hệ thống phát hiện xâm nhập mã nguồn mở và miễn phí trên Unix. Nó làm việc trên lớp mạng và lớp ứng dụng, nó có thể phát hiện các cuộc tấn công ẩn sử dụng lưu lượng được mã hóa hoặc những cố gắng né tránh phân tích và phát hiện [24].

D. Các công cụ phòng thủ

Chúng khác hơn so với IDS, chúng cũng sử dụng các kỹ thuật khác nhau để ngăn chặn các cuộc tấn công. Cơ chế và phương pháp khác nhau được sử dụng để phát hiện các mã độc hại và sau đó ngăn chặn các cuộc tấn công. Một số ví dụ về các hệ thống phòng chống xâm nhập (IPS) được liệt kê dưới đây:

• Intrusion Prevention System (IPS): là hệ thống ngăn ngừa xâm nhập, có chức năng theo dõi, ngăn ngừa kịp thời các hoạt động xâm nhập không mong muốn. Chức năng chính của IPS là xác định các hoạt động nguy hại, lưu giữ các thông tin này. Sau đó kết hợp với firewall để dừng ngay các hoạt động này, và cuối cùng đưa ra các báo cáo chi tiết về các hoạt động xâm nhập trái phép trên. Hệ thống IPS được xem là trường hợp mở rộng của hệ thống IDS, cách thức hoạt động cũng như đặc điểm của 2 hệ thống này tương tự nhau. Điểm khác nhau duy nhất là hệ thống IPS ngoài khả năng theo dõi, giám sát thì còn có chức năng ngăn chặn kịp thời các hoạt động nguy hại đối với hệ thống. Hệ thống IPS sử dụng tập luật giống như hệ thống IDS.

• Snort: là IDPS nổi tiếng và mạnh mẽ nhất, hoạt động trên lớp mạng và cũng có thể làm việc trên lớp ứng dụng. Nó có thể phát hiện và ngăn chặn các cuộc tấn công khác nhau như lỗi tràn bộ đệm, tấn công từ chối dịch vụ, tàng hình cổng quét, tấn công CGI, thăm dò SMB và các cuộc tấn công khác. Snort là công cụ mã nguồn mở được sử dụng rộng rãi và có nhiều nghiên cứu, phát triển cho nó [20].

• Suricata: là một hệ thống phát hiện và phòng chống xâm nhập mã nguồn mở và miễn phí. Nó hoạt động trên lớp ứng dụng để phát hiện và ngăn chặn các cuộc tấn công. Suricata chạy đa luồng làm cho nó nhanh hơn so với IPS và IDS khác. Các kỹ thuật phát hiện sử dụng bởi công cụ này được sử dụng dựa trên nguyên tắc bất thường [25].

• Firewall: là thiết bị phần cứng và/hoặc phần mềm giúp ngăn chặn một số liên lạc bị cấm bởi chính sách an ninh, dựa trên các bộ quy tắc. Một số loại tường lửa có thể hoạt động trên các lớp ứng dụng.

• Netfilter: là mã nguồn mở, được viết bằng ngôn ngữ C, và tường lửa miễn phí nhưng chỉ hoạt động trên Linux. Tường lửa này có thể được sử dụng với giao diện dòng lệnh. Nó hỗ trợ các giao thức khác nhau trên IPv4 và bao gồm các mô-đun khác nhau để xử lý các giao thức khác nhau [26].

• IPFilter hoặc "IPF" là một mã nguồn mở và tường lửa miễn phí. Nó hỗ trợ IPv4 và IPv6 và có thể làm việc trên các hệ điều hành như AIX, BSD/OS, DragonFlyBSD, FreeBSD, IRIX, HP-UX, Linux kernel, NetBSD, OpenBSD, OpenSolaris, QNX, Solarix, SunOS, và Tru46 [27]

E. Công cụ kiểm tra

Đây là những công cụ được sử dụng bởi cả Hacker và các chuyên gia kiểm thử xâm nhập. Sau đây là một số các công cụ kiểm tra thâm nhập quan trọng cho bộ giao thức TCP/IP.

• Nmap: là một công cụ quét, theo dõi và đánh giá bảo mật một hệ thống mạng được phát triển bởi Gordon Lyon [28]. Nmap là phần mềm mã nguồn mở miễn phí, ban đầu chỉ được phát triển trên nền tảng Linux sau đó được phát triển trên nhiều nền tảng khác nhau như Windows, Solari, Mac OS... và phát triển thêm phiên bản giao diện người dùng (zenmap).

• Netcat: là công cụ nhỏ và dễ sử dụng. Nó giúp thay đổi các gói tin để thử nghiệm các phản ứng giao thức [29].

• hping: là một công cụ mã nguồn mở và miễn phí dùng để phân tích các gói tin TCP/IP. Nó không có một giao diện người dùng đồ họa và chỉ có thể được truy cập bằng cách sử

 ISBN: 978-604-62-4226-0

dụng giao diện dòng lệnh. Nó hỗ trợ nhiều giao thức bao gồm ICMP, TCP, UDP và các giao thức RAW-IP [30].

IV. KẾT LUẬN

Bài viết này đã trình bày các dạng tấn công hướng vào khai thác các điểm yếu của bộ giao thức TCP/IP. Tác giả đã tập trung giới thiệu các công cụ, cơ chế xác định các lỗ hổng bảo mật có thể gây ra những cuộc tấn công và cách phòng chống chúng.

TÀI LIỆU THAM KHẢO

[1] Spafford, Eugene H. The internet worm incident. Springer Berlin Heidelberg, 1989.

[2] Chappell, Laura. "Inside the TCP Handshake." NetWare Connec- tion (2000).

[3] CERT, "CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks," September 1996.

[4] Tanase, Matthew. "IP spoofing: an introduction." Security Focus 11 (2003).

[5] Ferguson, Paul. "Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing." (2000).

[6] Heberlein, L. Todd, and Matt Bishop. "Attack class: Address spoofing."Proceedings of the 19th National Information Systems Security Conference. 1996.

[7] Trabelsi, Zouheir, and Khaled Shuaib. "NIS04-4: Man in the Mid- dle Intrusion Detection." Global Telecommunications Conference, 2006. GLOBECOM'06. IEEE. IEEE, 2006.

[8] Bellovin, Steven M. "A look back at." Computer Security Appli- cations Conference, 2004. 20th Annual. IEEE, 2004.

[9] Harris, B., and R. Hunt. "TCP/IP security threats and attack methods."Computer Communications 22.10 (1999): 885-897.

[10] Barbir, A., S. Murphy, and Y. Yang. "Generic threats to routing protocols." (2006).

[11] Yan, Boru, et al. "Detection and defence of DNS spoofing attack." Jisuanji Gongcheng/ Computer Engineering 32.21 (2006): 130-132.

[12] "Wireshark", online, www.wireshark.org. (last accessed on 25 May 2013)

[13] "TCPdump and libpcap", online, http://www.tcpdump.org/"

[14] "KISMET", online, http://www.kismetwireless.net

[15] "ETTERCAP", online, http://ettercap.github.io/ettercap

[16] "NESSUS vulnerability scanner", online, http://www.tenable.com/products/nessus

[17] "Open VAS- Open Vulnerability Assessment System", online, www.openvas.org (last accessed on 25 May 2013).

[18] "Core-impact", online, http://www.coresecurity.com/core- impact-pro (last accessed on 25 May 2013).

[19] "Retina NetworkSecurity Scanner", online, http://www.beyondtrust.com/Products/RetinaNetworkSecurityScanner

[20] Roesch, Martin. "Snort-lightweight intrusion detection for net- works."Proceedings of the 13th USENIX conference on System administration. 1999.

[21] Leach, John, and Gianni Tedesco. "Firestorm network intrusion detection system." Firestorm Documentation (2003).

[22] Zaraska, Krzysztof. "Prelude IDS: current state and development perspectives."URL http://www. prelude-ids. org/download/misc/pingwinaria/2003/paper. pdf(2003).

[23] Allan, Ant. "Enterasys Networks Dragon Intrusion Detection System (IDS)." (2002).

[24] Bro, I. D. S. "Homepage: http://www. bro-ids. org." (2013).

[25] "Suricata Intrusion Detection System", online, http://suricata-ids.org/

[26] Yao, Xiaoyu, and Chen ZHAO. "Research on Implementation and Application of Linux Kernel Firewall Netfilter [J]." Computer Engineering 8 (2003): 042.

[27] Reed, D.: IP Filter. Online. http://coombs.anu.edu.au/ avalon/ipfilter.html

[28] "Nmap", online, http://nmap.org/.

[29] "What is netcat?", online, http://netcat.sourceforge.net/

[30] "hping", online, http://www.hping.org/